



Secured Storage of Medical Records using Blockchain

Dr S P Abirami¹, Aathavan B², Bharathi A², Siddhaarth R², Mohan Raj G²

¹Assistant Professor, Department of Computer Science and Engineering,
Coimbatore Institute of Technology

²Undergraduate Student, Department of Computer Science and Engineering,
Coimbatore Institute of Technology

ABSTRACT

Fast digitization of health data has brought in new threats pertaining to the security, privacy, and overall integrity of such data. Centralized storage platforms are still vulnerable to data intrusions and unauthorized use. Blockchain technology can play a significant role in managing medical records because it is immutable and decentralized. This paper suggests Hyperledger Fabric and InterPlanetary File System (IPFS) to develop a blockchain based medical record management system that securely keeps entire access control, data integrity, and access provisioning policies intact. The proposed system is implemented securely by the application of cryptographic hashing, consensus, smart contracts, and other sophisticated mechanisms which all contribute towards making control more robust. The experiments carried out show that this method is successful in improving the privacy and security of healthcare information systems.

INTRODUCTION

Preserving health data in confidence and integrity is essential for both patient confidentiality and compliance with regulations. The existing hardware technologies for storing and processing healthcare information are centrally located servers that are susceptible to cyberattacks, unauthorized access and single points of failure. The frequency of rising data breaches in the healthcare sector over the past few years has created an imperative to create more secure and robust technologies.

Blockchain technology, with its immutable and decentralized ledger, offers an exciting alternative for maintaining data integrity, transparency, and security—sans central authority. Blockchain protects against unauthorized tampering by utilizing cryptographic hashing and consensus protocols, making patient records tamper-proof. Controlled and traceable access to medical data is also made possible by blockchain, helping to address critical issues regarding patient consent and adherence to global healthcare standards.

This study aims to develop a blockchain system for safely storing medical records using Hyperledger Fabric and IPFS. Hyperledger Fabric provides a permissioned blockchain network that can facilitate access control with efficient transactions. IPFS is employed to store medical records in a decentralized manner, alleviating the storage burden on the blockchain and making data available. The solution offered here is intended to enhance security, privacy, and interoperability in managing medical records, offering a scalable, compliant solution to the healthcare sector.

METHODOLOGY

The suggested system employs distributed storage and blockchain technology for secure storage of medical records. It has two major components:

Frontend Web Application: Built with React.js and Node.js, the user interface enables doctors to upload medical records and patients to view their own information safely.

Blockchain Network: Built with Hyperledger Fabric and CouchDB state database, it offers access control, keeps metadata (CID, doctor ID, patient ID, and reason for visit) and makes data immutable

Medical Record Upload:

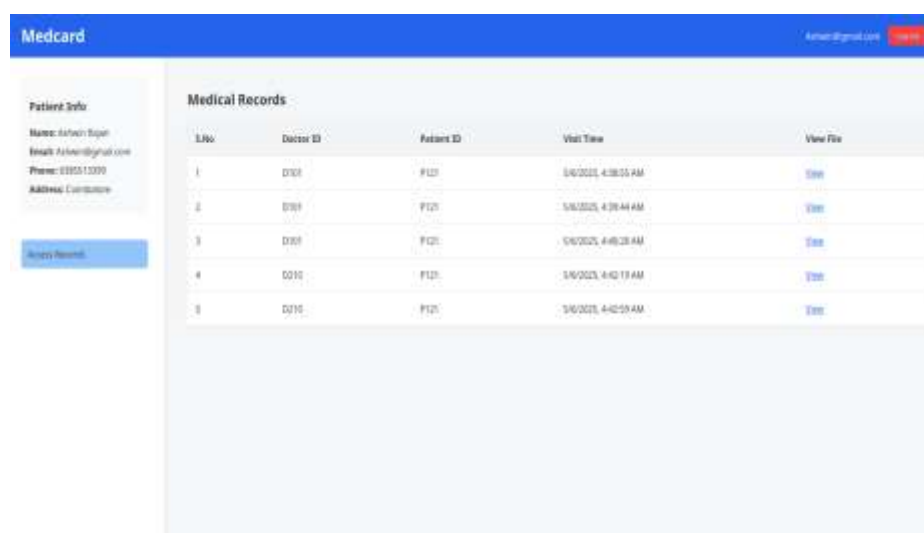
A doctor accesses the web portal, logs in, and adds a medical record by inputting the patient ID, reason for visit, and attaching the file. The record is first encrypted with AES to give data confidentiality at rest. The encrypted file is then posted on IPFS, which generates a Content Identifier (CID) — a hash pointer that addresses the file in a unique manner. Metadata (CID, patient ID, doctor ID, visit purpose) is sent to the blockchain network, wherein it is added as a transaction.



Figure 2.1 Uploading Medical Record

Patient Access:

Patients access the portal to view their records. Based on access policies that are embedded in smart contracts, patients can view only records that are for their ID. When a patient views a record, a transaction is saved on the blockchain to capture this act so that auditability and traceability can be ensured.



S.No.	Doctor ID	Patient ID	Visit Time	View File
1	D101	P121	1/4/2025, 4:38:55 AM	View
2	D101	P121	1/4/2025, 4:39:44 AM	View
3	D101	P121	1/4/2025, 4:40:28 AM	View
4	D101	P121	1/4/2025, 4:42:19 AM	View
5	D101	P121	1/4/2025, 4:42:59 AM	View

Figure 2.2 Patient Dashboard

IPFS Data Upload and CID Recovery:

Once the doctor uploads a health record (e.g., image, prescription, or diagnosis report) using the web interface, the document is client-side encrypted using AES to maintain the confidentiality of the data. The document is then uploaded to InterPlanetary File System (IPFS), a decentralized peer-to-peer distributed file system that is utilized for decentralized file management. Once uploaded successfully, IPFS creates a Content Identifier (CID) for the file. CID is a cryptographic hash that is an encoding of the file's contents — a smallest change in the file will result in a completely different CID. CID is an immutable, tamper-evident reference to a particular version of the file and is utilized for verification and retrieval.

Rather than storing the entire file onto the blockchain, this CID and other metadata such as patient ID, physician ID, visit reason, and timestamp are stored onto the Hyperledger Fabric blockchain. Patient or physician read requests thereafter result in retrieving the CID from the blockchain, then retrieving the matching file from IPFS, decryption, and presentation securely through web interface. This approach provides data integrity, decentralized availability, and secure access to sensitive medical information.



Figure 2.3 IPFS Dashboard

Blockchain Integration with Hyperledger Fabric:

After the CID of the uploaded medical record is fetched from IPFS, it is stored securely on the Hyperledger Fabric blockchain along with the corresponding metadata, including the Patient ID, Doctor ID, reason for visit. Hyperledger Fabric is an enterprise-focused permissioned blockchain platform and hence well-suited for handling sensitive healthcare information. Unlike public blockchains, it provides access control and identity management, with admission to membership of only the authorized ones (e.g., registered patients, certified doctors). Business rules are enforced through smart contracts, referred to as chaincode in Fabric, such as doctor identification verification, patient authorization verification, and logging of changes or access.

Every transaction that stores a CID or reports data access is digitally signed and appended to an immutable ledger, so that tampering with medical record history is rendered impossible. Furthermore, Fabric's modular architecture and pluggable consensus mechanism provide high throughput and scalability, so that the system can support many concurrent transactions. This blockchain layer provides the trusted audit trail, and it provides traceability, transparency, and tamper-proofing of all interaction associated with medical records.

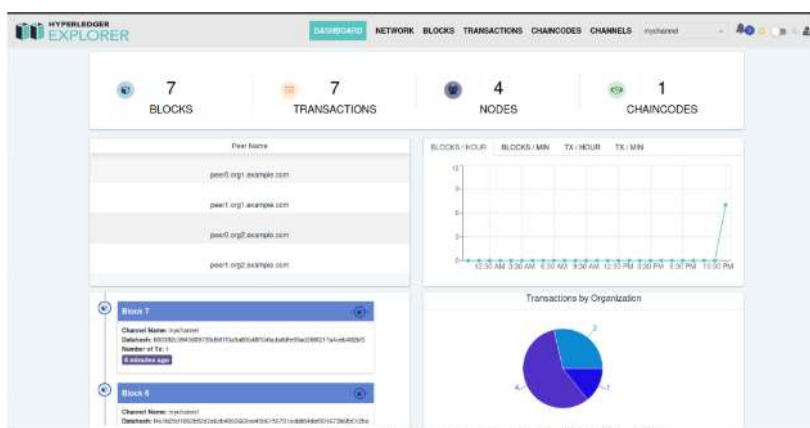


Figure 2.4 Hyperledger dashboard.

CouchDB in Blockchain Storage

To monitor the status of medical record transactions in our system, we use CouchDB as the Hyperledger Fabric state database. CouchDB is a key-value store that makes structured data easy to access and retrieve by storing key-value pairs in JSON format, including patient IDs and related IPFS CIDs. By enabling rich searches and indexing Users can be administrators, physicians, or patients, and each role has unique access rights:

Only the patient's own records are visible. Physicians have the ability to upload and view patient records. Administrators have complete authority, which includes controlling user access and monitoring system activity.

These roles serve to safeguard privacy and guarantee adherence to laws governing medical data., CouchDB enables the retrieval of metadata stored within it without requiring the reader to read the entire ledger. Particularly when there are numerous user activities and medical records, this is significantly faster.

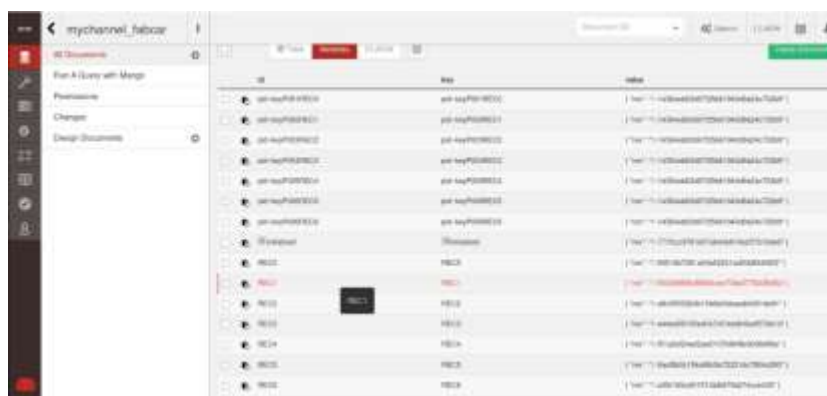


Figure 2.5 CouchDB Interface

Architecture:

This system is made to handle medical records in a transparent, safe, and user-friendly manner. To guarantee that medical data is securely stored and only accessible by authorized users, it combines decentralized storage (IPFS), blockchain technology (Hyperledger Fabric), and an understandable, role-based web interface.

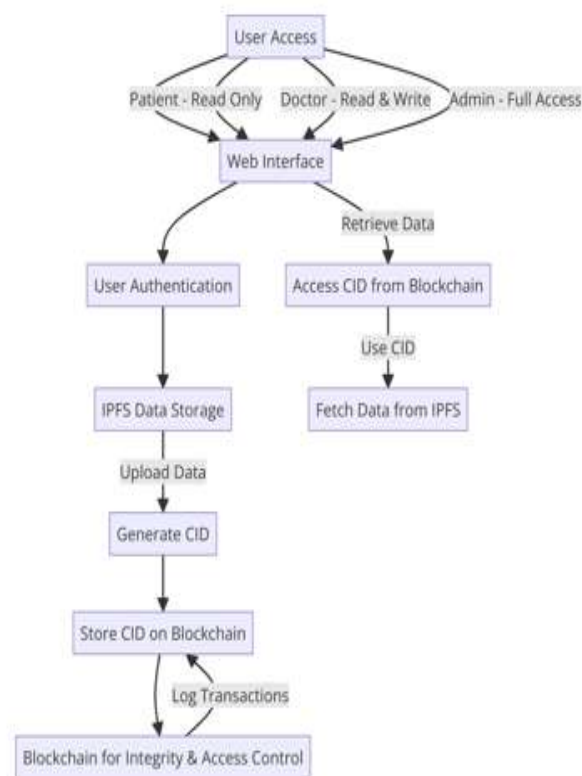


Figure 3.1 System Architecture

Role-Based Access

Users can be patients, doctors, or admins, and each role comes with specific access permissions:

Patients can only view their own records. Doctors can upload and access patient records. Admins have full control, including managing user access and overseeing system activity.

These role distinctions help protect privacy and ensure compliance with medical data regulations.



Figure 3.2 Role Based Access

Web Interface

Everyone uses a secure web portal to communicate with the system. Users can easily log in, upload, or retrieve records based on their permissions with this React-built interface.

Authentication First

The system verifies the user's identity before proceeding. Only verified users are permitted to continue through a secure login process that is powered by JWT (JSON Web Tokens). This guarantees that private medical information is never made available to unapproved users.

Uploading Medical Records

In order to protect patient confidentiality, a medical record uploaded by a doctor is first encrypted. This encrypted record then is stored in the InterPlanetary File System (IPFS); IPFS is a decentralized storage solution that works differently than traditional centralized servers. Once stored, IPFS returns a CID (Content Identifier) which is a unique hash that acts as the file's fingerprint.

The only thing that is required to access the file later on, while not compromising the contents of the file, is the CID.

RECORDING ON THE BLOCKCHAIN

After the CID is generated:

It is securely stored on the blockchain via smart contracts on Hyperledger Fabric. The system also records the individual that uploaded the file, the time, and the acquired role – cementing a transparent, tamper-proof record of the transaction.

This provides clarity surrounding ownership of the data and visible reduction of fraud or unauthorized alterations.

Accessing Medical Records

When a patient or provider wants to view a record:

The system refers to the blockchain to identify the correct CID of the requested file. Using that CID, the file can be fetched directly from IPFS. If the user has the appropriate permissions, the file is decrypted and rendered through the web interface.

This method allows to provide access at every step in a fast, secure, and controlled way.

Trust Through Blockchain

The blockchain layer adds benefits because it logs all activity and smart contracts enforce access rules so that only the right people can view or update data, and each action is traceable.

By combining integrity of blockchain, decentralized storage by IPFS and role based access control, we provide patients with comfort that their data is safe and provide doctors with the tools they need to provide timely care.

System Features

This system is developed with decentralization, removing any single point of failure and promoting the integrity of medical data. This system uses smart contracts to assure strict role-based access control to ensure that the Patient(s)



remain in control of who can read or alter their records. The system is protected against unauthorized change by design, while the immutability of blockchain technology provides a secure, traceable history for each medical record. The system included a component to use IPFS for the file storage component, which limits the blockchain load, improves scalability, while ensuring a high level of security, and operational efficiency.

The system implements HL7 standards, supporting communication with existing healthcare platforms, and ensuring interoperability, and smooth data exchange. An immutable audit tracking all access events, and data changes reinforces accountability and allows organizations to meet regulations. Security is improved through user authentication methods including multi-factor and biometric options. Having all these features provides a trusted user trust environment for sensitive healthcare data.

RESULTS AND DISCUSSION

The system was utilized in testing against synthetic medical data to validate functionality in areas such as security, access latency, and storage efficiency. The results were encouraging—by utilizing decentralized storage in the form of the IPFS, there was a marked decrease in the likelihood of a data breach, thus improving possible privacy and confidentiality of sensitive medical records. Accessing records was also quicker than other traditionally encrypted cloud storage models and served as demonstrate that the system can be effective in situations that resemble real-world use cases.

Despite these positives, there were a few limitations presented during the testing. the blockchain underlying component is secure and transparent, but there are scalability issues that could have performance implications based on how many users or records are onboarded. User onboarding - especially for non-blockchain type users - triggered some usability issues. These observations from testing clearly state that the secure and effective core system should address some usability issues and scalability if larger user populations are required.

Future Enhancements

The next stage of development will aim for a more intelligent, scalable, and user-centric system. The first enhancement will be the enablement of AI-based anomaly detection. This will help the system detect and identify unauthorized access attempts which will provide an alert feature. The AI anomaly detection built on predictive analytics will go a long way in the overall security of the system, since being able to identify potential threats prior to becoming so intrusive as to potentially impact the system will bolster the systems security.

The other improved features that will provide scale and ability will include cross-chain interoperability. The will allow secure medical data transfer across blockchain platforms which will allow the solution to be flexible within a myriad of healthcare environments. There will an additional secure mobile application developed to allow for real-time access to records for patients and doctors with security and authentication processes using biometrics such as fingerprint or face ID during mobile access.

Further exploration of enhancements will involve scalability, particularly the response improvements for smart contracts, as well as the capacity of the network to perform at an efficient level during higher transaction load volumes. There will be extension of the systems capability to facilitate integration with medical IoT from devices that will assist with the secure and real-time collection of health data for patient monitoring. Finally, to provide reliability and trust, the system will be maintained with routine updates to be compliant with evolving healthcare regulations and standards.

CONCLUSION

This study has demonstrated ways that blockchain and the IPFS together create a secure and reliable mechanism of storage for medical records by providing integrity, privacy, and access control.

Hyperledger Fabric's permissioned network restricts access and permissions to only the participants with access and IPFS provides a mechanism for distributing and storing the data on a scalable system.

The combination of these blockchain systems ensures compliance with healthcare standards while protecting the integrity of the data from tampering or unauthorized access.

The blockchain systems together also provide a decentralized solution that minimizes administrative overhead in tracking and managing medical information.

Future iterations of the system would seek to include enhanced scalability, interoperability and also AI-based security features.



These enhancements would help support broader adoption across a variety of healthcare platforms and a wider range of provider networks.

REFERENCES

Healthcare Record Management Using Blockchain - Pravesh Rana, Parth Dahiya, Nishant Suhag, Jagrat Singh - IJFMR Volume 5, Issue 5, September-October 2023. DOI 10.36948/ijfmr.2023.v05i05.6295

Deshpande, K. V., Patil, T., Nagare, S., Sarode, R., & Dhanke, A. (2023, June). MedNcrypt: A Blockchain based Decentralised Health Record Storage System using IPFS. In *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)* (pp. 1579-1587). IEEE.

Vasista, T. S., Singh, R. P., & Kumar, P. (2023, July). Advancing Healthcare: Unleashing the Potential of Cryptography, Blockchain, and Machine Learning. In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE

1. Control of Plant Growth by Monitoring Soil Moisture, Temperature and Humidity in Dry Climate, 2021, NK Madzhi and M A Nor Akhsan
2. Smart Automated Plant Monitoring System Using Blynk Application, 2023, Shefali Dhingra
3. Effect Of NPK Green Mix with Different Type of Manure on Spinach Growth and Yield
June 2023:IOP Conference Series Earth and Environmental Science 1182(1):012041
4. Effect of varieties and nutrient levels on growth, quality and nutrient uptake of palak (*Beta vulgaris* var. *Bengalensis*),2023: Ilal Khedkar, RK Sharma, SS Kushwah and Roshan Gallani- The Pharma Innovation
5. Monitoring of Soil Nutrients Using Soil NPK Sensor and Arduino L. Lenin Kumar, M. Srivani, Md. Tabassum Nishath, T. Akhil , Arugula Naveen and K. Charith Kumar, 2023:Ecology Environment and Conservation
6. Control of Plant Growth by Monitoring Soil Moisture, Temperature and Humidity in Dry Climate, 2021, NK Madzhi and M A Nor Akhsan
7. Smart Automated Plant Monitoring System Using Blynk Application, 2023, Shefali Dhingra